Software Engineering Institute

Improving the Security and Resilience of U.S. Postal Service Mail Products and Services Using the CERT® Resilience Management Model

Gregory Crabb, U.S. Postal Inspection Service
Julia H. Allen, Software Engineering Institute
Pamela D. Curtis, Software Engineering Institute
Nader Mehravari, Software Engineering Institute

January 2014

TECHNICAL NOTE
CMU/SEI-2013-TN-034

CERT® Division

http://www.sei.cmu.edu

Carnegie Mellon University

This material is based upon work funded and supported by the U.S. Postal Inspection Service and ODE under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the U.S. Postal Inspection Service or the United States Department of Defense.

This report was prepared for the
SEI Administrative Agent
AFLCMC/PZM
20 Schilling Circle, Bldg 1305, 3rd floor
Hanscom AFB, MA 01731-2125

DM-0000856

Table of Contents

List of Figures

List of Tables

Acknowledgments

The authors would like to thank Michael Ray, U.S. Postal Inspection Service, for his thoughtful review comments on this report.

Abstract

Developing and implementing measurable methodologies for improving the security and resilience of a national postal sector directly contribute to protecting the public and postal employees, assets, and revenues. Such methodologies also contribute to the security and resilience of the mode of transport used to carry mail and the protection of the global mail supply chain. Since 2011, the U.S. Postal Inspection Service (USPIS) has collaborated with the CERT® Division at Carnegie Mellon University's Software Engineering Institute to improve the resilience of selected U.S. Postal Service (USPS) products and services. The CERT Resilience Management Model (CERT-RMM) and its companion diagnostic methods have served as the foundational tool for this collaboration. CERT-RMM is a capability-focused maturity model for improving an organization's management of operational resilience activities across the domains of security management, business continuity management, and aspects of information technology operations management. These improvements enable high-value services to meet their missions consistently and with high quality, particularly during times of stress and disruption. This report describes the USPIS/CERT collaboration, how CERT-RMM has been applied to meet USPIS project objectives, how project outcomes are improving the resilience of USPS products and services, and how similar use of CERT-RMM applies to other transportation-systems subsectors.

1 Introduction

Since 2011, the U.S. Postal Inspection Service (USPIS) has collaborated with the CERT® Division at Carnegie Mellon University's Software Engineering Institute to improve the resilience of selected U.S. Postal Service (USPS) products and services.[1] This collaboration has included projects dealing with incident response, export screening, authentication services, physical security and aviation screening for international mail, Express Mail revenue assurance,[2] and development of mail-specific resilience management practices for mail induction, transportation, delivery, and revenue assurance. This report describes how USPIS and CERT staff have used the CERT Resilience Management Model (CERT-RMM) and mail-specific extensions to CERT-RMM to assess and improve safety and security capabilities and to identify and mitigate risks to revenue.

The authors believe that the USPIS application of CERT-RMM to ensuring the resilience of U.S. domestic and international mail from induction to delivery is likely applicable to other transportation sectors. This includes those sectors responsible for the movement of people and goods from one physical location to another, particularly when faced with disruption and stress to transportation services.

[1] CERT® is a registered mark of Carnegie Mellon University.

[2] The Express Mail product has been renamed Priority Mail Express since the time of the activities described in this report.

2 Background

2.1 USPS and USPIS

The USPS is rooted in a single, great principle: that every person in the United States—no matter who, no matter where—has the right to equal access to secure, efficient, and affordable mail service [USPS 2013]. This principle is supported by the mission of the USPIS, which is the law enforcement arm of the USPS. It is the longest standing federal law enforcement agency in the United States, dating back to 1772. The United States is the only country to have a separate and distinct postal inspection service. As the USPIS describes its purpose,

> *The mission of the U.S. Postal Inspection Service is to support and protect the U.S. Postal Service and its employees, infrastructure, and customers; enforce the laws that defend the nation's mail system from illegal or dangerous use; and ensure public trust in the mail.… Through its security and enforcement functions, the USPIS provides assurance to American businesses for the safe exchange of funds and securities through the U.S. Mail; to postal customers of the "sanctity of the seal" in transmitting correspondence and messages; and to postal employees of a safe work environment. [USPIS 2013]*

The USPIS is responsible for protecting the security of the USPS brand name, facilities, information, and technical assets. It enforces over 200 U.S. federal statutes addressing electronic crimes, mail fraud, mail theft, identity theft, child exploitation, and prohibited mailings such as bombs and biological and chemical threats.

USPIS Inspector in Charge of Revenue, Product, and Global Security Gregory Crabb has been the sponsor and proponent for the use of CERT-RMM within the USPS and the USPIS. He manages a number of programmatic efforts, including the investigation of cybercrime and revenue fraud. He also guides the development of secure USPS products. Crabb leads global security for the USPS, which includes being the liaison to global law enforcement and promoting more effective security controls through forums such as Interpol and the Universal Postal Union (UPU).

2.2 The CERT Resilience Management Model

CERT-RMM is a capability-focused maturity model for process improvement that reflects best practices from industry and government for managing operational resilience across the domains of security management, business continuity management, and aspects of information technology (IT) operations management. CERT-RMM defines operational resilience as "the emergent property of an organization that can continue to carry out its mission in the presence of operational stress and disruption that does not exceed its limit" [Caralli 2011]. Operational resilience is an organization's ability to protect its critical assets and keep essential services and processes operating, particularly during times of stress and disruption.

Through CERT-RMM, these best practices are integrated into a single model that provides an organization with a transformative path from a silo-driven approach for managing operational risk to an approach focused on achieving resilience management goals and supporting the organization's strategic direction. Practices focus on improving the organization's management of

key operational resilience processes. This improvement enables high-value services to meet their missions consistently and with high quality, in normal and adverse conditions [Caralli 2011].

CERT-RMM helps to ensure that the organization's important assets—people, information, technology, and facilities—effectively support business activities and services. The model serves as a foundation from which an organization can measure its current competency, set improvement targets, and establish plans and actions to close any identified gaps. As a result, the organization repositions and repurposes its security, business continuity, and IT operations activities and adopts a process improvement mindset that helps to keep services and assets productive in the long term [Allen 2012].

The model describes a process-based framework of goals and practices at four levels of increasing capability (Incomplete, Performed, Managed, and Defined) and a companion appraisal method. It comprises 26 process areas (PAs), shown in Figure 1, that define a set of practices that, when implemented collectively, satisfy a set of goals considered important for effectively managing the organization's ability to be operationally resilient [Caralli 2011].

Access Management	Measurement & Analysis
Asset Definition & Management	Monitoring
Communications	Organizational Process Focus
Compliance	Organizational Process Definition
Controls Management	Organizational Training & Awareness
Enterprise Focus	People Management
Environmental Control	Resilience Requirements Development
External Dependencies	Resilience Requirements Management
Financial Resource Management	Resilience Technical Solution Engineering
Human Resource Management	Risk Management
Identity Management	Service Continuity
Incident Management & Control	Technology Management
Knowledge & Information Management	Vulnerability Analysis & Resolution

Figure 1: CERT-RMM Process Areas

Users of the model select the PAs, specific goals, and specific practices that apply to a specific objective (such as those for the projects described in Sections 3–6 of this report) and ignore the rest. It is critical to identify which model content is most relevant based on the specific project need [Crabb 2012].

The following sections provide summaries of a diverse range of USPIS projects that have used CERT-RMM to respond to questions from senior leaders and to evaluate and improve USPS products and services. The report closes with a discussion of the potential applicability of CERT-RMM to the interests of other critical infrastructure organizations.

3 Early Applications of CERT-RMM to Help Meet USPIS Objectives

This section provides a series of short project summaries. Each of these projects served to increase USPIS understanding of CERT-RMM and the benefits that the organization could gain by applying it to specific security objectives for selected USPS products and services. Through insights and experiences gained during the CERT-RMM Users Group Workshop Series, the first project described, the USPIS Revenue, Product, and Global Security (RPGS) team recognized how they could apply goals and practices from the CERT-RMM model and its companion appraisal method to many of the challenges being addressed by the USPS and USPIS. Thus the Users Group was instrumental in informing the applications of CERT-RMM described in this report.

3.1 CERT-RMM Users Group

One role of the USPIS RPGS team is to investigate external computer security incidents targeted at the USPS and its customers and make recommendations to USPS Information Technology (IT) for information security improvements. From March 2011 through February 2012, members of this team participated in the first CERT-RMM Users Group Workshop Series [Allen 2012, SEI 2011b]. The purpose of the workshop series was to provide a forum for its members to implement a solution that met a specific resilience improvement objective tied to a USPIS organizational goal. Four 2-day workshops were conducted during this 12-month period, with assignments between workshops.

The improvement objective that the RPGS team selected was to improve its computer incident response and management processes, specifically incident identification, containment, eradication, and recovery. As a result of the workshop series, the RPGS team recommended the incorporation of law enforcement functions into existing USPS IT security policies. The RPGS team also developed a more comprehensive computer incident handling guide similar to those recommended by the U.S. National Institute of Standards and Technology (NIST) and the CERT Division.

In a July 2013 interview with *Federal Computer Week*, Crabb stated, “CERT-RMM helps us define the processes by which we conduct incident responses for security incidents, including how we interact with the other business units and the CISO’s [chief information security officer’s] office for the recovery of evidence and continuity of operations” [Joch 2013].

3.2 Export Screening

On a weekly basis, the USPS processes well over one million packages to overseas locations. The USPIS is responsible for assuring that mailers comply with specific export control requirements. By using CERT-RMM, the RPGS team was able to

- define objectives that an export screening program should meet
- identify relevant practices that apply to this compliance objective
- through awareness and training, provide a common language that helped all participating USPIS staff update their knowledge quickly

- objectively measure operational export screening performance against defined objectives

In a relatively short time frame, the RPGS team defined specific goals and practices that the USPS and USPIS needed to achieve and a project plan for doing so, defined work products to **g**uide decision making on what outputs to produce, and took a complex, overwhelming task and managed it using common criteria [Crabb 2012].

3.3 New Product Security Risk

The USPIS is often called upon to assess the risks associated with new products that the USPS is considering. CERT-RMM has proved useful in conducting such an assessment. For each new product being evaluated, the RPGS team selects relevant PAs and then applies CERT-RMM Risk Management goals and practices to each of these PAs for the new product, to aid in identifying risks and possible mitigation strategies. Using this approach for a specific product, the team develops strong risk statements by identifying asset-level risks for each practice area of interest. The team then develops a catalogue of risk statements for the new product and uses this information to present critical risk statements to the USPS portfolio product owner and other senior stakeholders such as the chief financial officer.

Based on these actions, decision makers are able to properly define and apply risk mitigation strategies. For one product assessment, this was accomplished in less than three business days, which would not have been possible without the use of CERT-RMM [Crabb 2012].

3.4 Defining Resilience Requirements for Authentication Services

In this project, the USPS enlisted CERT staff to help identify a complete set of resilience requirements for a new authentication service that was complex, network intensive, and internet facing. (Resilience requirements include protection requirements such as information security and privacy, and sustainment requirements such as availability, performance, continuity, and disaster recovery.) A CERT team evaluated the resilience requirements specified in the service's design document against NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST 2013], and identified a considerable number of additional controls needed. The team mapped the resulting resilience requirements by category to CERT-RMM PAs to facilitate using CERT-RMM to implement the requirements. The team also recommended using several other CERT-RMM PAs to support establishing effective governance for the new authentication service.

Sections 4–6 of this report provide more in-depth descriptions of several USPIS projects conducted during 2012 and 2013.

4 Assessing the Security Capability of International Postal Sector Organizations

The safety, security, and resilience of international postal and transportation critical infrastructure are vital to the global supply chain that enables worldwide commerce and communications. Security on an international scale continues to fail in the face of new and complex threats. This reality, together with the ever-increasing complexity of the global supply chain, calls for new and innovative approaches. Owners and operators of critical postal and transportation operations worldwide need new methods to identify, assess, and mitigate security risks and gaps in the most efficient and expedient manner possible.

The UPU, headquartered in Berne, Switzerland, is a unit of the United Nations that regulates the postal services of 192 member countries. These postal services form the largest physical distribution network in the world: "More than 5 million postal employees working in over 660,000 post offices all over the world handle an annual total of 434 billion letter-post items in the domestic service and 5.5 billion in the international service. More than 6 billion parcels are sent by post annually" [UPU 2013a].

For the past 17 years, the chief postal inspector of the USPIS has fulfilled a unique role with the UPU, which is to chair the Postal Security Group (PSG). The PSG's objective is to enhance the security of all operations within the worldwide postal sector. In early 2012, the UPU sponsored development of two standards for physical security and aviation screening. These were accepted and designated as mandatory at the 25th Universal Postal Congress in Doha, Qatar, in September 2012 [UPU 2013a]:

- *S58, Postal Security Standards – General Security Measures* defines the minimum physical and process security requirements applicable to critical facilities within the postal network [UPU 2013b].
- *S59, Postal Security Standards – Office of Exchange and International Airmail Security* defines minimum requirements for securing operations relating to the transport of international mail [UPU 2013c].

As a USPIS representative to the PSG, Crabb recognized the need for a simple, lightweight assessment method for determining the capabilities of postal organizations against the new standards. In a presentation to the UPU in February 2012, Crabb proposed several objectives that could be achieved through this effort [Gregory Crabb, unpublished data]:

- improve security practices (as participating organizations made whatever adjustments were revealed by the assessments as necessary to meet the standards)
- demonstrate assessed organizations' capabilities to regulators (the European Commission, the International Air Transport Association, the International Civil Aviation Organization, the World Customs Organization, and internal and external governance bodies)
- assess security suppliers
- have the PSG serve as the "independent validator" for the European Commission

Because of his team's experience with CERT-RMM, Crabb asked the CERT Division to develop such a method based on the CERT-RMM appraisal process, along with a companion field instrument with automated features. In February 2012, USPIS staff conducted the first pilot assessments using the new method against draft versions of S58 and S59. The USPIS continued to conduct assessments and work with CERT staff to improve the method throughout 2012. At the same UPU Congress in September 2012, this method was recognized as the approach for assessing compliance with the UPU standards.

Based on field reports, participating organizations have realized the following benefits from the assessment results:

- gained insight into the postal organization's capability by identifying the strengths and weaknesses of current security practices
- achieved recognition as having a strong security posture by the International Civil Aviation Organization, World Customs Organization, and supply chain partners that rely on postal services for moving goods
- obtained guidance to prioritize security-related improvement plans
- received feedback on the maturity level of the organization's security program
- were able to better identify and prioritize security risks

The USPIS, in its PSG leadership role, and postal sector organizations continue to use the assessment method today to achieve initial results and assess progress after implementing improvements. Additional project details are available in the report titled *A Proven Method for Identifying Security Gaps in International Postal and Transportation Critical Infrastructure* [Crabb 2013].

5 Development of Mail-Specific Resilience Management Practices

After experiencing the benefits of applying selected CERT-RMM PAs and practices to a range of USPIS challenges, in December 2011, Crabb asked CERT staff to develop one or more new PAs to manage the resilience of mail throughout its life cycle—from induction to delivery. The initial scope of this effort included mail acceptance, revenue confirmation, mail security, mail transport, and mail custody. The USPIS objectives for this project included the following [Crabb 2012, Joch 2013]:

- Define common criteria for assuring that USPS products are resilient.
- Evaluate business partners and customer operations in their handling of mail.
- Use these new PAs in conjunction with other selected CERT-RMM PAs to evaluate new and existing USPS products, services, suppliers, and partners, in terms of their security and resilience.
- Assure that each product's contribution to USPS revenue is commensurate with services delivered.
- Identify revenue collection gaps more quickly.

The development project commenced in January 2012 and was an active collaboration between USPIS subject-matter experts and CERT staff. The architecture of the mail-specific PAs follows that of the existing 26 PAs described in the CERT-RMM model. The scope and content of these PAs evolved significantly during the course of the development project. In July 2012, initial outlines for four mail-specific PAs—Mail Induction (MI), Mail Revenue Assurance (MRA), Mail Transportation (MT), and Mail Delivery (MD)—were accepted by the USPIS, as well as an initial draft of the MRA PA.

The PAs specific to the induction of mail and to mail revenue assurance were pilot tested extensively during the Express Mail projects described in Section 6. In April 2013, outlines for all four mail-specific PAs were accepted as baselined by the USPIS, and in July 2013, baselined versions of two complete PAs, MI and MRA, were accepted by the USPIS.

Table 1 describes these four PAs, their purposes, and some sample goals and practices.

Table 1: CERT-RMM Mail-Specific Process Area Purposes and Sample Goals and Practices

Process Area	Purpose	Goal/Practice	Practice
Mail Induction	Ensure that all mailpieces (mail) are inducted (collected and accepted) in accordance with USPS standards	Accept Mail practice	• Assist mailers in preparing mail according to standards • Refuse prohibited and improperly prepared mail • Verify eligibility of the mailpiece (type, class, extra services) • Perform acceptance scans • Ensure that each mailpiece is properly marked and endorsed • Ensure that correct payment for postage is made • Perform verification • Identify discrepancies

Process Area	Purpose	Goal/Practice	Practice
Mail Transportation	Ensure that all mailpieces (mail) are transported in accordance with USPS standards	Transport Mail and Screen Mail goals	• Sort mail for transportation • Prepare mail for transportation • Transport mail to destination processing facilities • Identify mail to be screened • Screen mail
Mail Delivery	Ensure that all mailpieces (mail) are delivered in accordance with USPS standards	Deliver Mail goal	• Sort mail for delivery • Prepare mail for delivery • Deliver mail
Mail Revenue Assurance	Ensure that the USPS is compensated for all mail that is accepted, transported, and delivered	Assure Mail Revenue goal	• Verify that postage affixed is sufficient • Verify that postage is not fraudulent • Verify receipt of payment for postage • Address mail revenue discrepancies

During the development project, the team identified four key resilience requirements for all mail that the USPS handles, as shown in Table 2.

Table 2: Four Key Resilience Requirements for U.S. Mail

Availability	The quality of mailpieces being accessible to all authorized citizens in a timely fashion as determined by the mail class. Mail must not be lost, stolen, or unnecessarily delayed.
Sanctity	The quality of mailpieces being inviolate (free from violation or damage; preserved from alteration of original content), intact (untouched by anything that causes harm or diminishes; no relevant component removed or destroyed) [Dictionary.com 2013, Merriam-Webster 2013]. Mailpieces must be kept in the condition intended for the sender and suitable for being transported by the USPS. Certain classes of mail must be protected against unauthorized access, modification, or disclosure.
Custody	The state of mailpieces being in the immediate charge and control of authorized USPS personnel from induction through delivery.
Visibility	The ability to determine the progress of mail through the mailstream to ensure on-time delivery [USPS 2011].

Each PA addresses goals and practices to achieve these resilience requirements. One or more of these requirements may also apply to other types of assets and goods that are transported from one location to another.

The USPIS RPGS team, with assistance from CERT staff, has begun to employ the practices in the MRA and MI PAs to evaluate the current USPS processes and practices associated with mail acceptance and revenue assurance activities for Express Mail (see Section 6.1) and to assure that the USPS is adequately compensated for all Express Mail services and mailpieces (see Section 6.2). These activities have resulted in identifying opportunities to improve the resilience of Express Mail practices, data to inform risk mitigation planning for Express Mail revenue, investigative leads, and improvements to the MRA and MI PAs.

6 Express Mail Project

The USPIS RPGS team chose the Express Mail (EM) product for the first direct application of the newly developed mail-specific PAs, MRA and MI. There had been a number of indications of fraud and revenue loss in the EM channel, such as counterfeit Information-Based Indicia (digital markings on mail that denote postage payment). The USPIS decided to use MRA and MI to try to determine how extensive these types of problems are and how well USPS processes, practices, and controls work for catching them.

The USPIS engaged the CERT Division to lead an appraisal of Express Mail using selected MRA and MI practices and others from CERT-RMM. The purpose of the appraisal was to identify and evaluate gaps in current USPS processes and practices associated with EM induction and revenue assurance activities. Using information collected in the appraisal, the CERT team then developed an instrument that allows a USPIS postal inspector to examine EM operations at a facility and identify EM revenue risks.

6.1 Express Mail Appraisal

A CERT team used the CERT-RMM Class C capability appraisal methodology [SEI 2011a] to conduct the appraisal. A Class C appraisal involves the collection of evidence through observation, interviews, and examination of artifacts such as documenation, forms, and reports. It results in characterizations of the extent to which the *intent* of each practice is realized (high, medium, or low), statements about strengths and weaknesses found, and improvement recommendations. The practices selected for evaluation in the EM appraisal concerned

- standards, activities, and systems in place that support EM revenue assurance during verification, acceptance, and processing
- standards, activities, and systems in place to ensure that the USPS is compensated for EM
- requirements, controls, and monitoring in place to address risks to EM revenue from meter vendors, online printable postage vendors, and Web Tools users
- measurement objectives and capabilities in place for supporting EM revenue assurance
- the use of training in support of EM revenue assurance
- USPS activities for identifying and strategically managing risks to EM revenue

As part of the discovery process, the appraisal team visited the Morgan Processing and Distribution Center, the James A. Farley Station, and the JFK Facility in New York City for tours, observations, interviews, and meetings with USPS personnel. Further appraisal activities were conducted at USPS headquarters in Washington, DC.

The results of the appraisal enabled the USPIS and the CERT team to identify practice and control issues to focus on more in-depth verification in the next phase of the project.

6.2 Express Mail Revenue Risk Identification

For the second phase of the Express Mail project, the CERT team developed an assessment instrument for USPIS postal inspectors and revenue fraud analysts to use to examine and evaluate

EM operations at USPS facilities. The instrument enables further verification of the risks to EM revenue that were identified in the appraisal. The assessed facility can use the insight obtained to inform improvement efforts locally, and the USPS can use it to inform decisions about how to target efforts to reduce risks of EM revenue loss across the postal system. The assessments also may bring to light cases that require further investigation.

The assessment instrument contains scripted questions that relate directly to practices in the MI and MRA PAs about EM revenue risks such as unaccepted EM, shortpaid EM, and use of fraudulent postage. Inspectors are also instructed to look for any steps taken and technologies used to try to prevent or detect those risks and steps taken when any of those types of revenue loss actually occur. Inspectors capture the anomalies that they observe, statements from interviews, and results of follow-up inquiries or investigations that they initiate.

For each question, using guidance supplied in the assessment instrument, inspectors then consider the evidence and characterize the extent to which the facility implements the practice implicit in the question. For example, at processing and distribution centers, EM clerks are asked, “Do you look for EM pieces that have not been accepted?” This question relates to the MI practice about accepting and verifying mail according to USPS standards. Inspectors make characterizations for questions using the FILIPINI scale: Fully Implemented, Largely Implemented, Partially Implemented, or Not Implemented. Next, inspectors roll up question characterizations into practice characterizations, using a set of rules to characterize an implementation as High, Medium, Low, or Not Applicable for each practice from the collective FILIPINI results of all the questions related to the practice. Inspectors submit their results to USPIS headquarters, where the characterizations and other information, such as the number of investigative leads generated, are aggregated and analyzed.

Enterprise-wide deployment (through local use of the instrument, including at all five International Service Centers) has enabled the USPIS to make progress toward doing sufficient analysis to support national observations about Express Mail revenue risk and to move forward in a longer term transition to an automated, database-driven approach to risk analysis. Some topics that the RPGS team hopes to address in the near term include determining the importance of EM relative to other revenue risks, how much EM revenue is attributable to specific geographic regions, the frequency and financial impact of EM fraud, which types of EM are more susceptible to fraud, and ways to reconcile payment with automated methods.

7 Applicability of CERT-RMM to Other Transportation Subsectors

There are strong interrelationships between postal, shipping, and transportation critical infrastructures when it comes to security, safety, and resilience. This fact is emphasized in U.S. Presidential Policy Directive 21 (PPD-21), *Critical Infrastructure Security and Resilience*, which was issued by the president on February 12, 2013 [White House 2013]. The updated structure of the nation's critical infrastructure sectors, which PPD-21 put in place, combines postal, shipping, and transportation functions into a single, overarching critical infrastructure sector. Table 3 summarizes the list of subsectors in the restructured transportation sector and their key characteristics of relevance to operational resilience.

Table 3: U.S. Transportation Sector and Its Subsectors

Transportation Subsectors	Primary Units of Transportation	Modes of Transportation
Aviation	People and goods	Air
Highway Infrastructure and Motor Carrier	People and goods	Ground
Maritime Transportation Systems	People and goods	Sea
Mass Transit and Passenger Rail	People	Ground
Pipeline Systems	Oil and gas	Ground
Freight Rail	Goods	Ground
Postal and Shipping	Mailpieces and goods	Air, ground, and sea

The concept of operational resilience, its management, and many of the techniques embedded in CERT-RMM and utilized by the USPS and the USPIS also directly apply to all subsectors of the restructured transportation sector, as illustrated in Table 4.

Table 4: Applicability of Transportation Subsectors to USPS/USPIS Projects

Transportation Subsectors	Incident Response	Export Screening	Authentication Services	Physical Security	Revenue Assurance Risk
Aviation	X	X	X	X	X
Highway Infrastructure and Motor Carrier	X			X	X
Maritime Transportation Systems	X	X	X	X	X
Mass Transit and Passenger Rail	X		X	X	X
Pipeline Systems	X			X	X
Freight Rail	X		X	X	X
Postal and Shipping	X	X	X	X	X

Whether it is people, physical goods, oil and natural gas, or mailpieces that are being moved from one location to another, stakeholders in all transportation subsectors are concerned about similar operational risks and interested in the same set of core security, safety, and resilience requirements (e.g., availability, sanctity, custody, and visibility).

8 Future Plans and Summary

One of the ongoing initiatives that the USPIS RPGS team hopes will produce significant results is the automation of measures to reduce mail fraud and to ensure that the USPS is compensated for all mail that it accepts, transports, and delivers. The RPGS team plans to implement revenue assurance as defined by the new mail-specific MRA PA. The team is using CERT-RMM to develop new measurement and monitoring activities for examining revenue resilience by defining performance reporting capabilities against these activities. One planned project is to develop a relative risk rating for each customer. The risk rating is intended to help the USPIS examine what each organization represents to the USPS from a fraud perspective. Using this rating, the USPIS can apply procedures to identify criminal misconduct and reduce relative risk by applying appropriate control procedures [Crabb 2013]. Another aspect of measurement and monitoring includes approaches for managing diverse data stores that provide visibility on aspects of revenue and the ability to examine certain revenue types, risks to these, and ways to measure risk, for example, by type of financial or mailpiece transaction.

On a regular basis, the RPGS team uses CERT-RMM to plan and develop an effective response to specific situations such as those described in this report. USPS and USPIS business units have developed a strong appreciation for the work products that are generated by using this model [Crabb 2012]. CERT-RMM gives USPS and USPIS staff a common set of goals and terminology that helps coordinate resilience efforts. “You are not going to win if you don’t have your security professionals—and, in my case, law enforcement officers—on the same page relative to how resilience should be managed,” Crabb said in a *Federal Computer Week* article [Joch 2013]. A successful resilience strategy can spotlight policy gaps before they become a problem and help agencies make decisions about how to allocate resources effectively.

USPS and USPIS experiences demonstrate that the resilience management framework and the associated techniques offered by CERT-RMM enable a structured, repeatable, and integrated approach for owners, operators, and regulators of critical transportation infrastructures and subsectors. This approach enables more effective planning, assessment, management, and sustainment of transportation products and services to ensure that they meet all required security, safety, and resilience needs, particularly when faced with disruption and stress.

In addition to applications at the USPS and USPIS, principles and practices of operational resilience codified in CERT-RMM have been successfully used to meet the resilience and cybersecurity needs of other critical infrastructure sectors. Examples include the U.S. Department of Energy’s Electricity Subsector Cybersecurity Capability Maturity Model [DoE 2012], the U.S. Department of Homeland Security’s Cyber Resilience Review [DHS 2012], and Lockheed Martin Corporation’s Corporate Business Resiliency Program [David 2011].

References

URLs are valid as of the publication date of this document.

[Allen 2012]
Allen, J. H. & Young, L. R. *Report from the First CERT-RMM Users Group Workshop Series* (CMU/SEI-2012-TN-008). Software Engineering Institute, Carnegie Mellon University, April 2012. http://www.sei.cmu.edu/library/abstracts/reports/12tn008.cfm

[Caralli 2011]
Caralli, R. A.; Allen, J. H.; & White, D. W. *The CERT Resilience Management Model: A Maturity Model for Managing Operational Resilience*. Addison-Wesley, 2011.

[Crabb 2012]
Crabb, G. *U.S. Postal Inspection Service Use of the CERT Resilience Management Model* (CERT podcast). Software Engineering Institute, Carnegie Mellon University, August 2012. http://www.cert.org/podcast/show/20120821crabb.html

[Crabb 2013]
Crabb, G.; Allen, J. H.; Curtis, P. D.; & Mehravari, N. *A Proven Method for Identifying Security Gaps in International Postal and Transportation Critical Infrastructure*. U.S. Postal Inspection Service, August 2013.

[David 2011]
David, W.; Mehravari, N.; & White, D. W. "Application of the CERT Resilience Management Model at Lockheed Martin." Presented at the 2011 Software Engineering Process Group North America Conference, Portland, OR, March 2011. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=19352

[DHS 2012]
U.S. Department of Homeland Security. *Cyber Resilience Review*. DHS, 2012. http://www.ahrmm.org/ahrmm/news_and_issues/issues_and_initiatives/files/ahrmm_cyber_resilience_review_032712.pdf

[Dictionary.com 2013]
Dictionary.com. "Inviolate" and "Intact." http://dictionary.reference.com (2013).

[DoE 2012]
U.S. Department of Energy. *Electricity Subsector Cybersecurity Capability Maturity Model*. DoE, May 2012. http://energy.gov/oe/downloads/electricity-subsector-cybersecurity-capability-maturity-model-may-2012

[Joch 2013]
Joch, A. "Operational Resilience: Bringing Order to a World of Uncertainty." *Federal Computer Week*, July 8, 2013. http://fcw.com/articles/2013/07/08/exectech-operational-resilience.aspx

[Merriam-Webster 2013]
Merriam-Webster. “Inviolate” and “Intact.” http://www.merriam-webster.com/dictionary (2013).

[NIST 2013]
National Institute of Standards and Technology. *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST Special Publication 800-53, Revision 4). NIST Computer Security Division, Information Technology Laboratory, April 2013. http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf

[SEI 2011a]
Software Engineering Institute. *CERT Resilience Management Model Capability Appraisals.* SEI, April 2011. http://www.cert.org/resilience/rmm_appraisals.html

[SEI 2011b]
Software Engineering Institute. *CERT Resilience Management Model (CERT-RMM) Users Group Workshop Series*. SEI, 2011. http://www.sei.cmu.edu/training/p92.cfm

[SEI 2013]
Software Engineering Institute. http://www.sei.cmu.edu (2013).

[UPU 2013a]
Universal Postal Union. *Postal Security Standards*. http://www.upu.int/en/activities/postal-security/security-standards.html (2013).

[UPU 2013b]
Universal Postal Union. *Postal Security Standards: General Security Measures* (S58). UPU, July 2013. http://www.upu.int/uploads/tx_sbdownloader/standardS58PostalSecurityEn.pdf

[UPU 2013c]
Universal Postal Union. *Postal Security Standards: Office of Exchange and International Airmail Security* (S59). UPU, July 2013. http://www.upu.int/uploads/tx_sbdownloader/standardS59PostalSecurityEn.pdf

[USPIS 2013]
U.S. Postal Inspection Service. *Mission*. https://postalinspectors.uspis.gov/aboutus/mission.aspx (2013).

[USPS 1999]
Historian, United States Postal Service. *Postal Service Mission and “Motto.”* USPS, October 1999. http://about.usps.com/who-we-are/postal-history/mission-motto.pdf

[USPS 2011]
United States Postal Service. *Glossary of Postal Terms* (Publication 32). USPS, April 2011. http://about.usps.com/publications/pub32.pdf

[USPS 2013]
United States Postal Service. *Delivering the Mail and More*. http://about.usps.com/who-we-are/postal-history/delivering-mail.htm (2013).

[White House 2013]
White House, Office of the Press Secretary. *Presidential Policy Directive – Critical Infrastructure Security and Resilience* (Presidential Policy Directive/PPD-21). White House, February 12, 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	January 2014	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Improving the Security and Resilience of U.S. Postal Service Mail Products and Services Using the CERT® Resilience Management Model	FA8721-05-C-0003

6. AUTHOR(S)

Gregory Crabb (U.S. Postal Inspection Service), Julia H. Allen, Pamela D. Curtis, and Nader Mehravari

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2013-TN-034

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFLCMC/PZE/Hanscom Enterprise Acquisition Division 20 Schilling Circle Building 1305 Hanscom AFB, MA 01731-2116	n/a

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

Developing and implementing measurable methodologies for improving the security and resilience of a national postal sector directly contribute to protecting the public and postal employees, assets, and revenues. Such methodologies also contribute to the security and resilience of the mode of transport used to carry mail and the protection of the global mail supply chain. Since 2011, the U.S. Postal Inspection Service (USPIS) has collaborated with the CERT® Division at Carnegie Mellon University's Software Engineering Institute to improve the resilience of selected U.S. Postal Service (USPS) products and services. The CERT Resilience Management Model (CERT-RMM) and its companion diagnostic methods have served as the foundational tool for this collaboration. CERT-RMM is a capability-focused maturity model for improving an organization's management of operational resilience activities across the domains of security management, business continuity management, and aspects of information technology operations management. These improvements enable high-value services to meet their missions consistently and with high quality, particularly during times of stress and disruption. This report describes the USPIS/CERT collaboration, how CERT-RMM has been applied to meet USPIS project objectives, how project outcomes are improving the resilience of USPS products and services, and how similar use of CERT-RMM applies to other transportation-systems subsectors.

14. SUBJECT TERMS	15. NUMBER OF PAGES
CERT-RMM, resilience management, risk assessment, risk mitigation, shipping security, transportation security, mail security	29

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL